UNITED STATES DISTRICT COURT

for the

District of New Mexico

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

INSTAGRAM USERNAMES @pbeck666777; @pbeck1234789; @hypnotripdj; @boss.glass THAT IS STORED BY META PLATFORMS INC

Case No. 22-MR-993

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See attachment A, attached hereto and incorporated herein.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See attachment B, attached hereto and incorporated herein.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 2261A	Stalking

The application is based on these facts:

See Affidavit, attached hereto and incorporated herein

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Eric Bruce
Applicant's signature

Eric Bruce, Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone *(specify reliable electronic means)*.

Date: June 24, 2022

Karen B Molzen

City and state: Albuquerque, New Mexico

Karen B. Molzen, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW MEXICO

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH: Instagram Usernames: @pbeck666777; @pbeck1234789; @hypnotripdj; @boss.glass THAT IS STORED AT PREMISES CONTROLLED BY META PLATFORMS, INC. (FORMERLY FACEBOOK, INC.)	Case No. 22-MR-993 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Eric Bruce, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises controlled by Meta Platforms, Inc. (formerly Facebook, Inc.), an online communications provider headquartered at 1601 Willow Road, Menlo Park, California.

2. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Meta Platforms, Inc. to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

3. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been since January, 2019. While employed by the FBI, I have investigated federal criminal violations related to high technology or cybercrime. I have gained experience through training

and everyday work relating to conducting these types of investigations. Prior to becoming a Special Agent of the FBI, I earned Bachelor's degrees in Mathematics and Economics and a Master's degree in International Affairs. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. § 2261A, and I am authorized by the Attorney General to request a search warrant.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, law enforcement officers, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that evidence of violations of 18 U.S.C. § 2261A (Stalking) exists in the Instagram accounts @pbeck666777, @pbeck1234789, @hypnotripdj, and @boss.glass (collectively, the SUBJECT ACCOUNTS). There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

Background & Terms

1. **IP Address**: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

2. 18 U.S.C. § 2261A criminalizes conduct by which someone "with the intent to kill, injure, harass, [or] intimidate…uses the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce, or any other facility of interstate or foreign commerce to engage in a course of conduct that…places that person in reasonable fear of the death of or serious bodily injury or…causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress." A "course of conduct" is described as "two or more acts, evidencing a continuity of purpose".

Summary of Investigation to Date

3. On or about May 7, 2022, I identified a complaint filed by DW, a resident of Texas, with the Internet Crime Complaint Center (IC3). The IC3 is a government organization that supplies the public with a reporting mechanism to provide information to the FBI regarding suspected internet-facilitated criminal activity. In the complaint, DW alleged she was being stalked, harassed, and threatened by Patrick Beck, a resident of Albuquerque, New Mexico. DW

alleged Beck used online social media to send her threatening and harassing messages as well as make public posts about her.

4. I communicated with DW via email regarding the complaint. DW further explained that BECK had been "catfished" online by someone using her publicly available photos. I understand the term "catfish" to refer to the use of photos belonging to another person to trick someone into an online relationship. DW was a model on Instagram and made pictures of herself publicly available. According to DW, BECK identified her real accounts, became obsessed with her, and believed they had been married. DW did not know BECK and did not have a relationship with him. When DW told BECK to stop contacting her, BECK started sending harassing and threatening messages. This conduct continued for approximately a year. DW also explained that her friend, DW2[1], a resident of Michigan, had become the target of abuse as well.

5. Following my communication with DW, I identified a complaint, filed by DW2 on or about February 8, 2022, with the FBI's National Threat Operations Center (NTOC). in the complaint, DW2 alleged that BECK targeted him because he was associated with DW on social media. DW2 alleged BECK had threatened DW2 and DW2's family with injury, death, and rape starting in February 2022. DW2 further alleged BECK had posted personal details about DW2 using multiple social media accounts including DW2's address, phone number, family members, and photos along with messages imploring others to injure and/or harass DW2 and DW2's family.

[1] DW2 is a person, known to the FBI, who bears the same initials as complainant DW but bears no familial relationship to DW.

6. On or about May 18, 2022, DW2 contacted me by phone and informed me that DW had died, apparently of suicide, some days prior. DW2 opined BECK's ongoing harassment of DW may have contributed to her suicide.

7. I obtained and reviewed a driver's license photograph of BECK on or about May 25, 2022 from the FBI Albuquerque operations center.

8. Between approximately May 7, 2022 and June 3, 2022, DW2 communicated with me via email and provided me with numerous screenshots of messages and social media posts allegedly made by BECK using several Instagram accounts, several of which appeared to have been created for the purpose of sending messages to DW2. In many of the messages, the user of the account(s) alleges that DW2 initiated the harassment, a fact which DW2 denied in email communications to me. DW2 further indicated that he uses Instagram to promote his woodworking business and many of the harassing messages were publicly posted as comments to his business posts.

9. On or about June 2, 2022, I reviewed the screenshots provided by DW2 and identified the SUBJECT ACCOUNTS. In the following sections, DW and DW2's names are redacted from representations of the Instagram posts and messages. DW's name and related information is redacted in blue and DW2's name and related information is redacted in red.

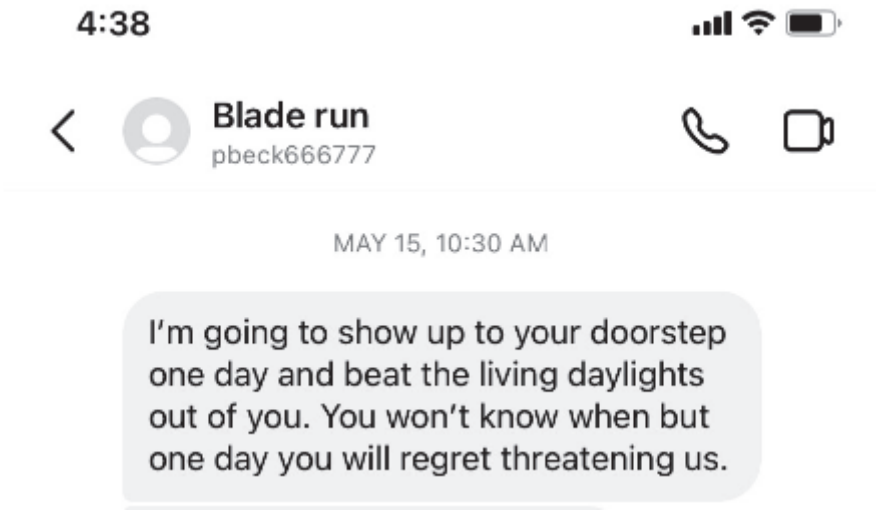
DETAILS OF INSTAGRAM ACCOUNT @pbeck666777

10. On or about June 2, 2022, I reviewed screenshots of communications provided by DW2 purportedly showing direct messages sent from the Instagram account @pbeck666777 to DW2 and identified the following representative messages:

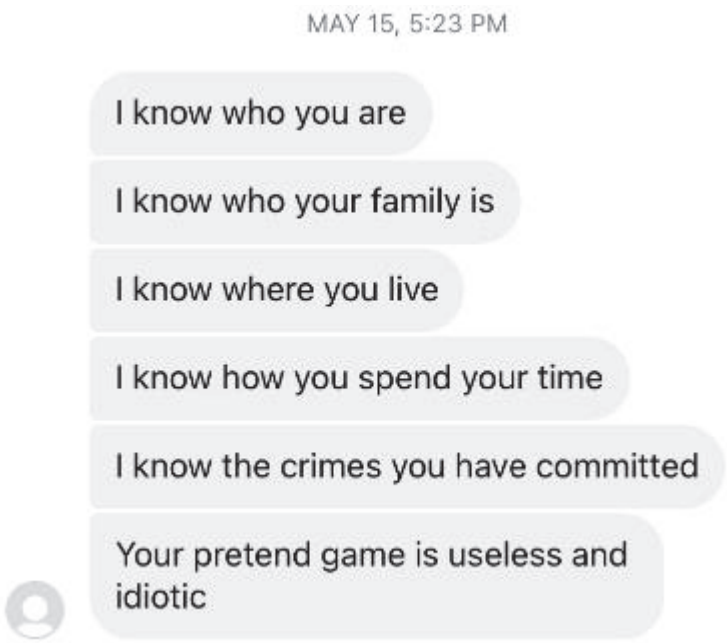
a.


MAY 6, 3:20 PM
Replied to your story
Only you can see this
You are retarded.
Fuck you
you are a piece of shit. If you think I'm letting what you did to me slide you have another thing coming
loek I don't remember what you did you fucking nasty hateful disgusting piece of shit
fuck you
im getting revenge on all of you like I did the last time

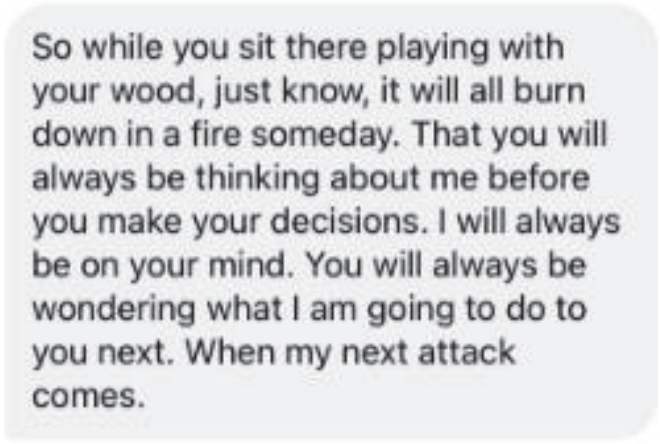
b.


4:38
Blade run
pbeck666777
MAY 15, 10:30 AM
I'm going to show up to your doorstep one day and beat the living daylights out of you. You won't know when but one day you will regret threatening us.

c.



d.



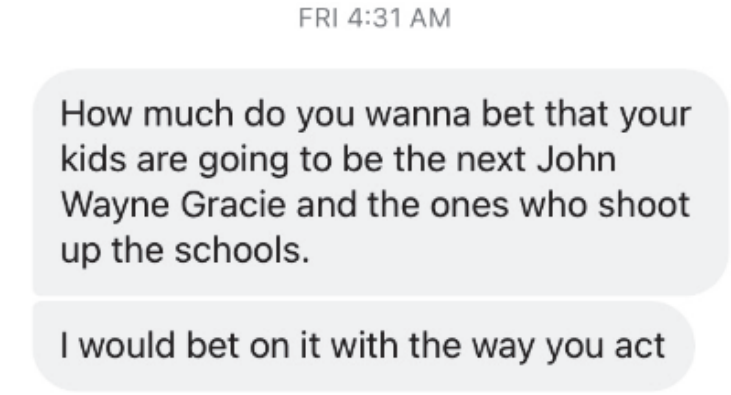
11. I identified dozens of similar messages sent from this account to DW2 over the course of approximately eleven days in May 2022. Of note, it appears the messages were sent unsolicited and that DW2 replied only once, requesting the sender stop messaging and posting pictures of him and his family. Based on the content of these messages, I have probable cause to believe that evidence of violations of 18 U.S.C. 2261A exists in the account @pbeck666777.

DETAILS OF INSTAGRAM ACCOUNT @pbeck1234789

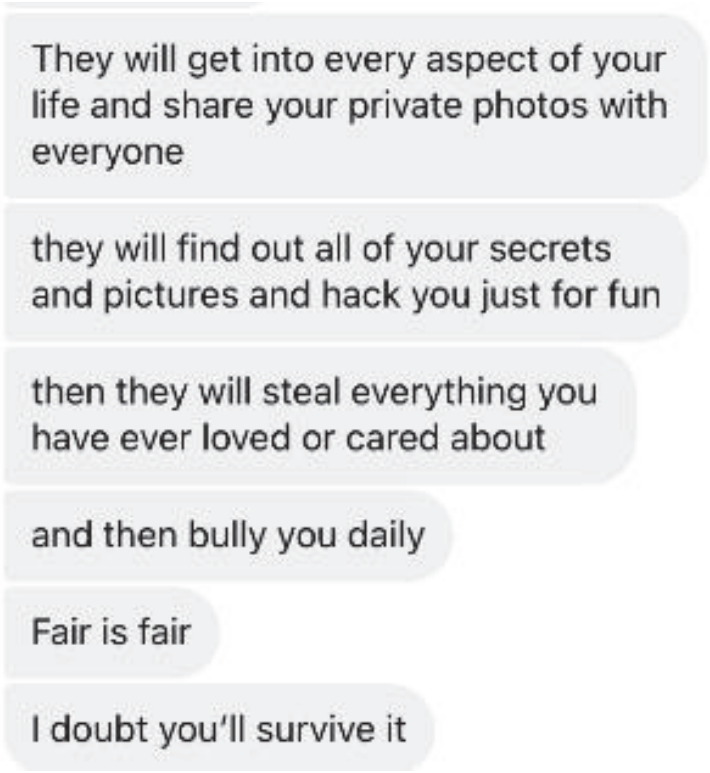
12. On or about June 2, 2022, I reviewed screenshots of communications provided by DW2 purportedly showing direct messages sent from the Instagram account @pbeck1234789 to DW2 and identified the following representative messages:

a.

b.



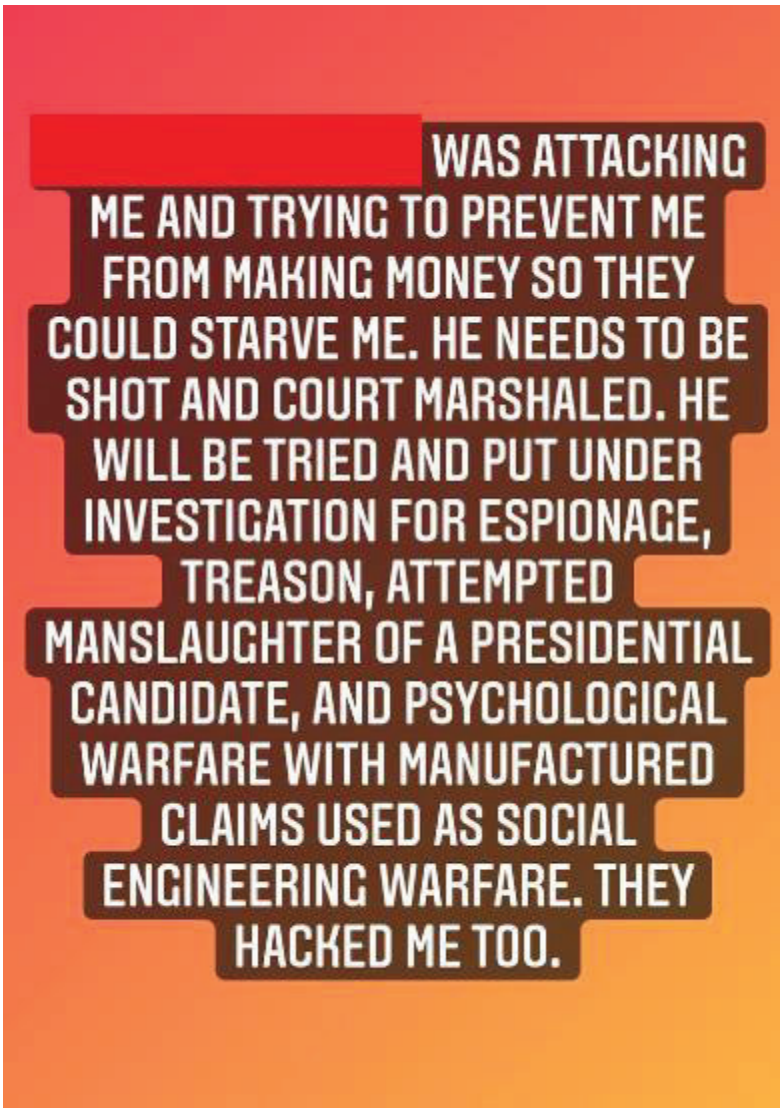
c.



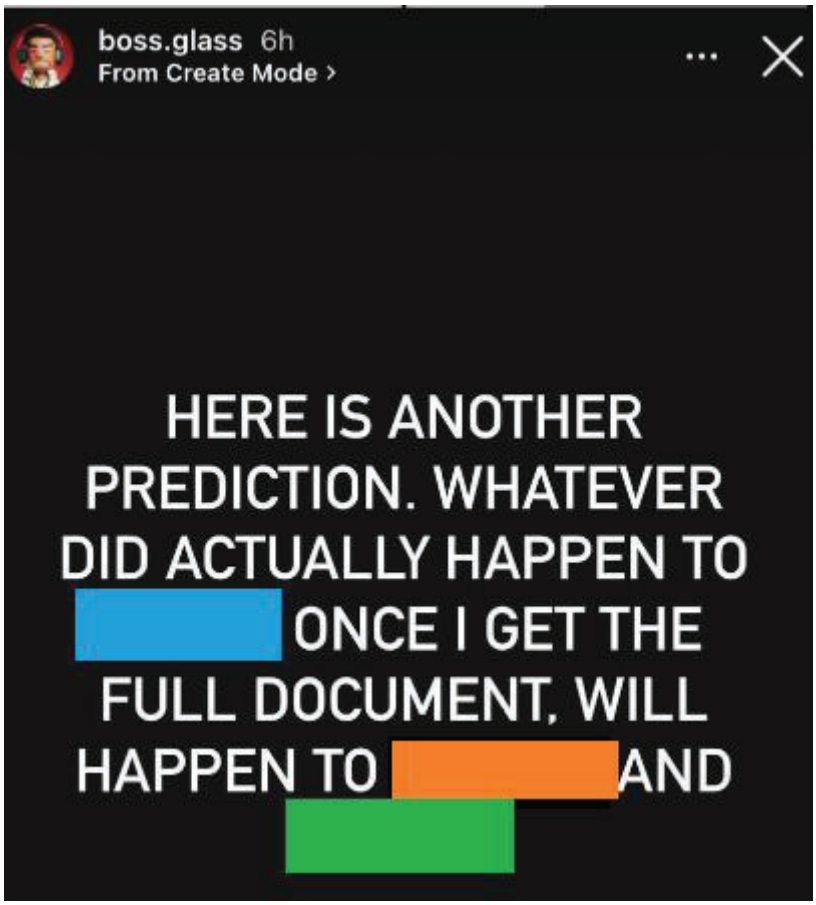
13. I identified dozens of similar direct messages sent from this account to DW2 over the course of approximately 10 days in May 2022. I observed the messages appeared to have been initiated by the user of the account @pbeck1234789 with minimal reply from DW2. Based on the content of these messages, I have probable cause to believe that evidence of violations of 18 U.S.C. 2261A exists in the account @pbeck1234789.

DETAILS OF INSTAGRAM ACCOUNT @boss.glass

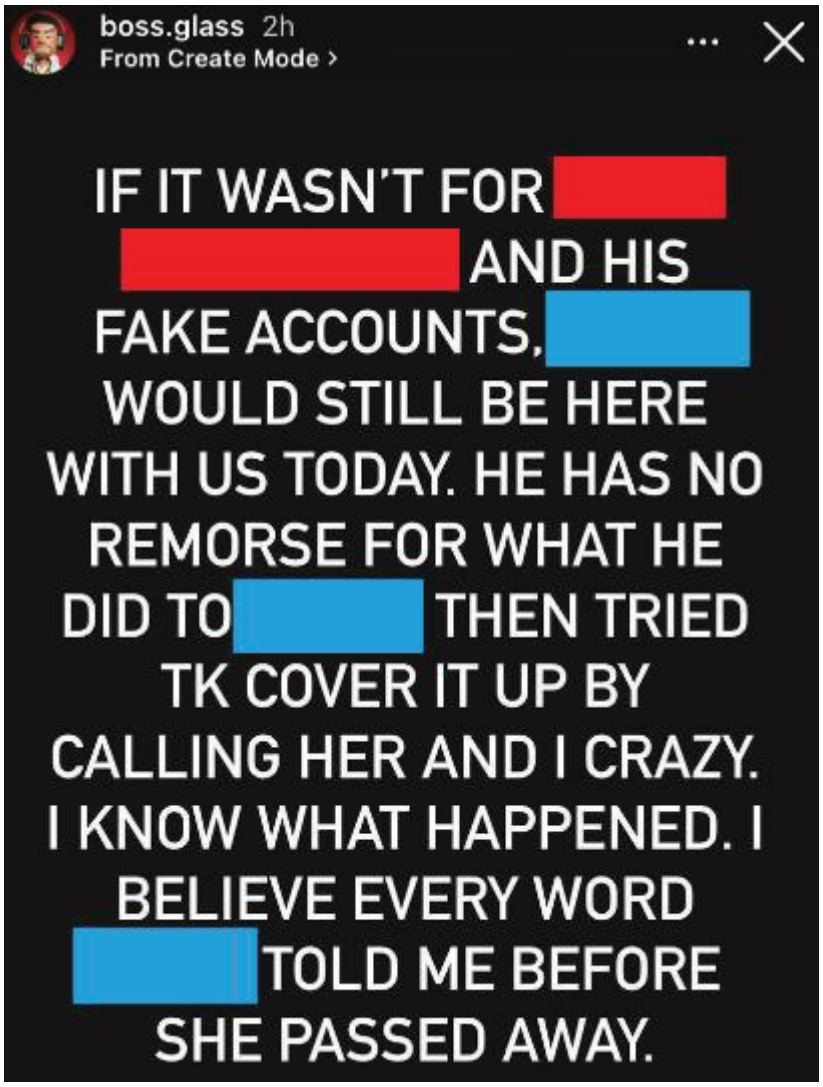
14. On or about June 2, 2022, I reviewed screenshots of communications provided by DW2 purportedly showing messages sent from the Instagram account @boss.glass to DW2 and identified the following representative messages:

a. 

i. According to DW2, this message was posted February 28, 2022. In a follow-up email, DW2 clarified this message was posted by @boss.glass on Instagram.

b. 

i. According to DW2, this message was publicly posted on May 30, 2022 following DW's death. [Note: The names of two other known victims are redacted in green and orange from this representation of the screenshot provided by DW2].

c. 

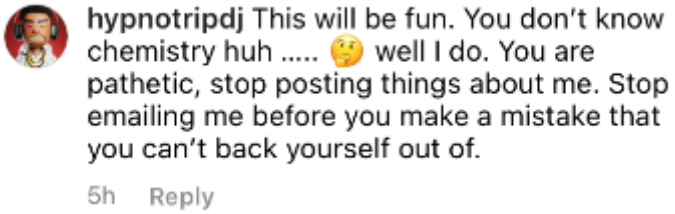
i. According to DW2, this message was posted May 30, 2022 following DW's death.

15. On or about June 1, 2022, I reviewed posts on the public facing profile for the account @boss.glass and identified several pictures posted by the user of the account that appeared to depict Beck based on my review of BECK's New Mexico driver's license picture.

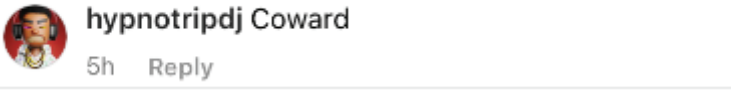
16. Based on the content of these messages, I have probable cause to believe that evidence of violations of 18 U.S.C. 2261A exists in the account @boss.glass.

DETAILS OF INSTAGRAM ACCOUNT @hypnotripdj

17. On or about June 2, 2022, I reviewed screenshots of communications provided by DW2 purportedly showing messages sent from the Instagram account @hypnotripdj to DW2 and identified the following representative messages:

a. 

i. According to DW2, this message was posted as a reply to one of DW2's business posts on May 11, 2022.

b. 

i. According to DW2, this message was posted as a reply to one of DW2's business posts on May 11, 2022.

18. On or about June 1, 2022, I reviewed posts on the public facing profile for the account @hypnotripdj and identified several pictures posted by the user of the accounts that appeared to depict BECK based on my review of BECK's New Mexico driver's license picture. Several of these pictures were the same as those posted to the account @boss.glass.

19. Based on the content of these messages and the public photos indicating BECK was the user of the account, I have probable cause to believe that evidence of violations of 18 U.S.C. 2261A exist in the account @hypnotripdj.

SUMMARY

20. Based on my training and experience, I know that online communication providers, like Instagram, collect information regarding the users of such communication

accounts that may tend to identify the user of the accounts. I also know that a comprehensive review of the contents of such accounts may provide valuable context regarding the intent of users sending and receiving communications that may either inculpate or exculpate the sender of the messages.

BACKGROUND CONCERNING INSTAGRAM[2]

21. Instagram is a service owned by Meta Platforms, Inc. (formerly Facebook, Inc.), a United States company and a provider of an electronic communications service as defined by 18 U.S.C. §§ 3127(1) and 2510. Specifically, Instagram is a free-access social networking service, accessible through its website and its mobile application, that allows subscribers to acquire and use Instagram accounts, like the target accounts listed in Attachment A, through which users can share messages, multimedia, and other information with other Instagram users and the general public.

22. Meta Platforms, Inc. collects basic contact and personal identifying information from users during the Instagram registration process. This information, which can later be changed by the user, may include the user's full name, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, credit card or bank account number, and other personal identifiers. Facebook keeps records of changes made to this information.

23. Meta Platforms, Inc. also collects and retains information about how each user accesses and uses Instagram. This includes information about the Internet Protocol ("IP")

[2] The information in this section is based on my training and experience, and on information published by Facebook on its website and its Instagram website, including, but not limited to, the following webpages: "Data Policy," available at https://help.instagram.com/519522125107875; "Information for Law Enforcement," available at https://help.instagram.com/494561080557017; and "Help Center," available at https://help.instagram.com.

addresses used to create and use an account, unique identifiers and other information about devices and web browsers used to access an account, and session times and durations.

24. Each Instagram account is identified by a unique username chosen by the user. Users can change their usernames whenever they choose but no two users can have the same usernames at the same time. Instagram users can create multiple accounts and, if "added" to the primary accounts, can switch between the associated accounts on a device without having to repeatedly log-in and log-out.

25. Instagram users can also connect their Instagram and Facebook accounts to utilize certain cross-platform features, and multiple Instagram accounts can be connected to a single Facebook account. Instagram accounts can also be connected to certain third-party websites and mobile apps for similar functionality. For example, an Instagram user can "tweet" an image uploaded to Instagram to a connected Twitter account, post it to a connected Facebook account, or transfer an image from Instagram to a connected image printing service. Meta maintains records of changed Instagram usernames, associated Instagram accounts, and previous and current connections with accounts on Facebook and third-party websites and mobile apps.

26. Instagram users can "follow" other users to receive updates about their posts and to gain access that might otherwise be restricted by privacy settings (for example, users can choose whether their posts are visible to anyone or only to their followers). Users can also "block" other users from viewing their posts and searching for their accounts, "mute" users to avoid seeing their posts, and "restrict" users to hide certain activity and prescreen their comments. Instagram also allows users to create a "close friends list" for targeting certain communications and activities to a subset of followers.

27. Each Instagram user has a profile page where certain content they create and share ("posts") can be viewed either by the general public or only the user's followers, depending on privacy settings. Users can customize their profile by adding their name, a photo, a short biography ("Bio"), and a website address.

28. One of Instagram's primary features is the ability to create, edit, share, and interact with photos and short videos. Users can upload photos or videos taken with or stored on their devices, to which they can apply filters and other visual effects, add a caption, enter the usernames of other users ("tag"), or add a location. These appear as posts on the user's profile. Users can remove posts from their profiles by deleting or archiving them. Archived posts can be reposted because, unlike deleted posts, they remain on Facebook's servers.

29. Users can interact with posts by liking them, adding, replying to comments, or sharing them within or outside of Instagram. Users receive notification when they are tagged in a post by its creator or mentioned in a comment (users can "mention" others by adding their username to a comment followed by "@"). An Instagram post created by one user may appear on the profiles or feeds of other users depending on a number of factors, including privacy settings and which users were tagged or mentioned.

30. An Instagram "story" is similar to a post but can be viewed by other users for only 24 hours. Stories are automatically saved to the creator's "Stories Archive" and remain on Facebook's servers unless manually deleted. The usernames of those who viewed a story are visible to the story's creator until 48 hours after the story was posted.

31. Instagram allows users to broadcast live video from their profiles. Viewers can like and add comments to the video while it is live, but the video and any user interactions are

removed from Instagram upon completion unless the creator chooses to send the video to IGTV, Instagram's long-form video app.

32. Instagram Direct, Instagram's messaging service, allows users to send private messages to select individuals or groups. These messages may include text, photos, videos, posts, videos, profiles, and other information. Participants to a group conversation can name the group and send invitations to others to join. Instagram users can send individual or group messages with "disappearing" photos or videos that can only be viewed by recipients once or twice, depending on settings. Senders can't view their disappearing messages after they are sent but do have access to each message's status, which indicates whether it was delivered, opened, or replayed, and if the recipient took a screenshot. Instagram Direct also enables users to video chat with each other directly or in groups.

33. Instagram offers services such as Instagram Checkout and Facebook Pay for users to make purchases, donate money, and conduct other financial transactions within the Instagram platform as well as on Facebook and other associated websites and apps. Instagram collects and retains payment information, billing records, and transactional and other information when these services are utilized.

34. Instagram has a search function which allows users to search for accounts by username, user activity by location, and user activity by hashtag. Hashtags, which are topical words or phrases preceded by a hash sign (#), can be added to posts to make them more easily searchable and can be "followed" to generate related updates from Instagram. Facebook retains records of a user's search history and followed hashtags.

35. Meta Platforms, Inc. collects and retains location information relating to the use of an Instagram account, including user-entered location tags and location information used by Facebook to personalize and target advertisements.

36. Meta Platforms, Inc. uses information it gathers from its platforms and other sources about the demographics, interests, actions, and connections of its users to select and personalize ads, offers, and other sponsored content. Meta Platforms, Inc. maintains related records for Instagram users, including information about their perceived ad topic preferences, interactions with ads, and advertising identifiers. This data can provide insights into a user's identity and activities, and it can also reveal potential sources of additional evidence.

37. In some cases, Instagram users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Meta Platforms, Inc. typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

38. For each Instagram user, Meta Platforms, Inc. collects and retains the content and other records described above, sometimes even after it is changed by the user (including usernames, phone numbers, email addresses, full names, privacy settings, email addresses, and profile bios and links).

39. In my training and experience, evidence of who was using Instagram and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to

establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

40. Based on my training and experience, direct messages, photos, and videos are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to an Instagram account may provide direct evidence of the offenses under investigation and can also lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

41. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Meta Platforms, Inc. can indicate who has used or controlled the Instagram account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, messaging logs, documents, photos, and videos (and the data associated with the foregoing, such as geolocation, date and time) may be evidence of who used or controlled the account at a relevant time, and device identifiers and IP addresses can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

42. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting accounts information in an effort to conceal evidence from law enforcement).

43. Other information connected to the use of an account may lead to the discovery of additional evidence. For example, accounts are often assigned or associated with additional identifiers such as account numbers, advertising IDs, cookies, and third-party platform subscriber identities. This information may help establish attribution, identify and link criminal activity across platforms, and reveal additional sources of evidence.

44. Therefore, Meta Platforms, Inc.'s servers are likely to contain stored electronic communications and information concerning subscribers and their use of Instagram. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

45. Based on the aforementioned information and investigation, it is reasonable to believe that the SUBJECT ACCOUNTS will contain records and evidence of violations of 18 U.S.C. § 2261A including harassing or threatening messages, the identity of the user of the accounts, and additional context regarding the messages. Moreover, it is reasonable to search the contents of The SUBJECT ACCOUNTS for evidence of stalking as well as for information corroborating the identity of the user(s) of the SUBJECT ACCOUNTS and their state of mind regarding intent.

46. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Meta Platforms, Inc. who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

47. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

Eric Bruce
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to me via telephone or other reliable electronic means on June 24, 2022, 2022

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

This warrant applies to information associated with Instagram accounts @pbeck666777, @pbeck1234789, @hypnotripdj, and @boss.glass (collectively, the SUBJECT ACCOUNTS), that is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc. (formerly Facebook, Inc.), a company headquartered at 1601 Willow Road, Menlo Park, California.

KBM

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Meta Platforms, Inc. ("Meta")

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Meta, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Meta is required to disclose the following information to the government for each account or identifier listed in Attachment A:

A. All business records and subscriber information, in any form kept, pertaining to the account, including:

1. Identity and contact information (past and current), including full name, e-mail addresses, physical address, date of birth, phone numbers, gender, hometown, occupation, websites, and other personal identifiers;
2. All Instagram usernames (past and current) and the date and time each username was active, all associated Instagram and Facebook accounts (including those linked by machine cookie), and all records or other information about connections with Facebook, third-party websites, and mobile apps (whether active, expired, or removed);
3. Length of service (including start date), types of services utilized, purchases, and means and sources of payment (including any credit card or bank account number) and billing records;

KBM

4. Devices used to login to or access the account, including all device identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, and apps and web browsers;

5. All advertising information, including advertising IDs, ad activity, and ad topic preferences;

6. Internet Protocol ("IP") addresses used to create, login, and use the account, including associated dates, times, and port numbers, from January 2021 to present;

7. Privacy and account settings, including change history; and

8. Communications between Meta and any person regarding the account, including contacts with support services and records of actions taken;

B. All content (whether created, uploaded, or shared by or with the account), records, and other information relating to videos (including live videos and videos on IGTV), images, stories and archived stories, past and current bios and profiles, posts and archived posts, captions, tags, nametags, comments, mentions, likes, follows, followed hashtags, shares, invitations, and all associated logs and metadata, from January 2021 to present;

C. All content, records, and other information relating to communications sent from or received by the account from January 2021 to present, including but not limited to:

1. The content of all communications sent from or received by the account, including direct and group messages, and all associated multimedia and metadata, including deleted and draft content if available;

2. All records and other information about direct, group, and disappearing messages sent from or received by the account, including dates and times, methods, sources and destinations (including usernames and account numbers), and status (such as delivered, opened, replayed, screenshot);

3. All records and other information about group conversations and video chats, including dates and times, durations, invitations, and participants (including usernames, account numbers, and date and time of entry and exit); and

4. All associated logs and metadata;

D. All content, records, and other information relating to all other interactions between the account and other Instagram users from January 2021 to present, including but not limited to:

1. Interactions by other Instagram users with the account or its content, including posts, comments, likes, tags, follows (including unfollows, approved and denied follow requests, and blocks and unblocks), shares, invitations, and mentions;

2. All users the account has followed (including the close friends list), unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow, and of users who have followed, unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow the account;

3. All contacts and related sync information; and

4. All associated logs and metadata;

KBM

E. All records of searches performed by the account from January 2021 to present; and

F. All location information, including location history, login activity, information geotags, and related metadata from January 2021 to present.

Meta is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. § 2261A, those violations involving Patrick BECK, DW, DW2, or other persons yet unidentified, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Threats to harm or injure;

(b) Communications that would cause, attempt to cause, or be reasonably expected to cause substantial emotional distress;

(c) Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;

(d) Evidence indicating the account owner's state of mind as it relates to the crime under investigation;

(e) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

KBM

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS

PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Meta, and my official title is _____. I am a custodian of records for Meta. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Meta, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Meta.; and

c. such records were made by Meta as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature

KBM